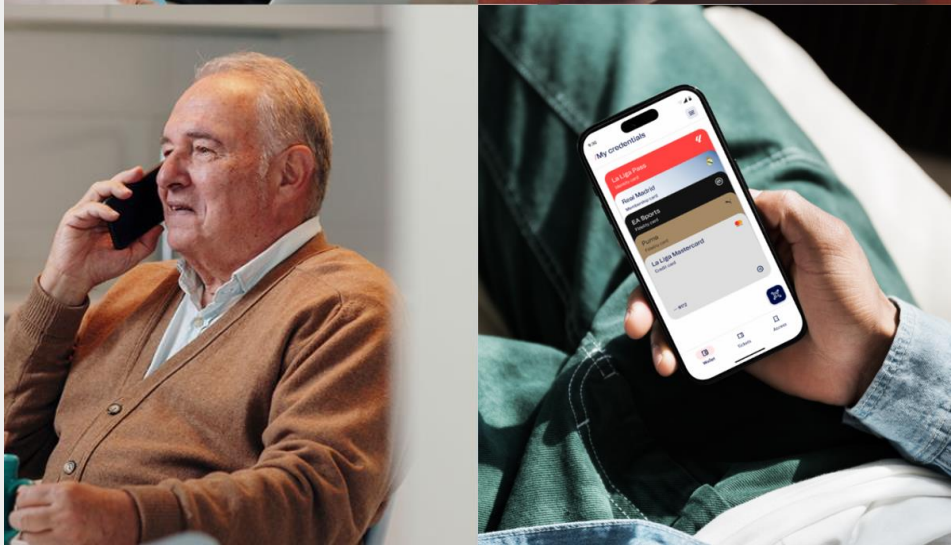
/Del Fraude a la Confianza: La Identidad Digital como pilar de la Administración Pública

Ciberseguridad, centralidad del dato
y el Wallet de Identidad para
la transformación digital

VeriDas

SOCINFO digital



/Un/a ciudadano/a, cientos de verificaciones de identidad

SALUD / SERVICIOS SOCIALES

Acceso a la Historia Clínica Electrónica
Solicitud de cita médica en el sistema de salud público
Expedición y renovación de la tarjeta sanitaria
Acceso a recetas electrónicas y medicamentos
Registro y acceso a programas de asistencia social
Verificación de identidad para ayudas a la dependencia
...

EDUCACIÓN

Matrícula en centros educativos públicos
Solicitud de becas y ayudas al estudio
Acceso a plataformas digitales de educación
Inscripción en formación profesional o cursos públicia
...

HACIENDA PÚBLICA

Presentación de declaraciones fiscales
Pago y gestión de impuestos autonómicos (IBI, sucesiones, etc.)
Acceso a la sede electrónica tributaria
Solicitud de aplazamientos o fraccionamientos de pago
...

REGISTRO CIVIL

Solicitud de certificados de nacimiento, matrimonio o defunción
Expedición de certificados de empadronamiento
Registro y cambios en el domicilio oficial
...

PARTICIPACIÓN CIUDADANA

Votación en consultas ciudadanas y presupuestos participativos
Acceso a portales de transparencia y datos abiertos
Solicitud y firma de documentos electrónicos en la sede digital
Participación en plataformas de quejas y sugerencias
...

EMPLEO Y SEGURIDAD SOCIAL

Registro como demandante de empleo en el servicio autonómico
Solicitud de subsidios o ayudas al desempleo
Acceso a cursos de formación para desempleados
Verificación para la firma de contratos con entidades públicas
...

VIVIENDA, SEGURIDAD, JUSTICIA, TRÁFICO...

Fraude de identidad

/Ciberataques contra Administración Pública española

1 cada 3 minutos

Solo durante esta charla, 5 ciberataques

/IA Generativa
La democratización del fraude

EL CORREO

Detienen en Bilbao a un hombre por suplantar la identidad de otro para que percibiera ayudas sociales desde Senegal

La cantidad estafada asciende a 56.000 euros y se encontraba dado de alta en la Seguridad Social y trabajando para una empresa ubicada en Basauri

España

ELECCIONES CATALUÑA · ANDALUCÍA · CATALUÑA · COMUNIDAD VALENCIANA · GALICIA · MADRID · PAÍS VASCO

ACTUALIDAD POLÍTICA Puigdemont cierra la puerta a pactar con el PSC e insta a ERC a que diga si votará a Illa

ESTAFA >

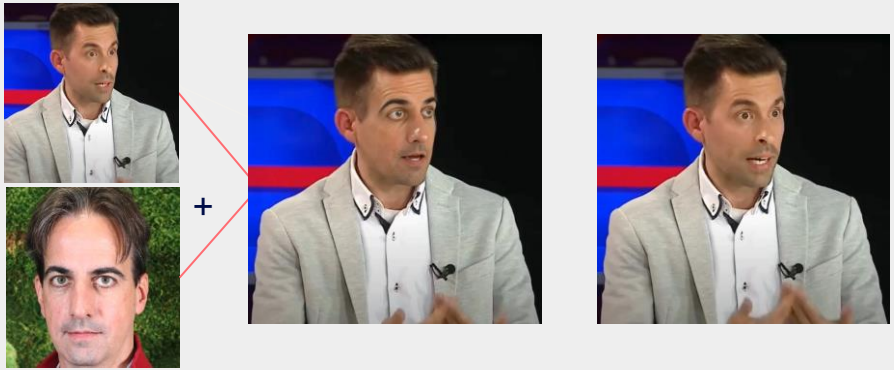
Un hombre estafa más de un millón de euros en ayudas sociales en Bizkaia con 62 identidades falsas

La operación de la Policía Nacional se salda con la detención de 23 personas que participaban en la red

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



/La analogía del fraude en moneda

Primera fotocopiadora inventada por Chester Carlson

1938

IBM fabrica la primera impresora matricial de punto

1958

Hewlett Packard crea la primera impresora de inyección de tinta

1976

Primera impresora láser de menos de $1.000

1990

Primer dispositivo láser multifunción para el gran público.

1998

Años 40

Hilo de seguridad incrustado en papel con un patrón

Años 50

Billetes que reaccionan a la luz ultravioleta.

Años 70

Microimpresión. Texto difícil de reproducir con precisión.

Años 80

Elementos holográficos. Cambian de apariencia cuando se inclina el billete.

Años 90

Tintas ópticamente variables. Cambian de color dependiendo del ángulo de visión.

/Fraude de identidad en el entorno digital y presencial

Fraude real detectado en los últimos 6 meses (global)

Reemplazo de foto
4%

Ataque a pantalla
4%

Ataque de impresión
3%

Menor de edad
1%

Documento caducado
1%

No hay coincidencia entre el selfie y la foto del documento
1%

¿Es consciente de que esto ocurre en sus procesos de onboarding? ¿Lo detectas?

/Fraude de identidad en el entorno digital y presencial

🚨 Casos reales de fraude de identidad detectados en España ⚠️

EJEMPLO REAL

Un solo individuo, múltiples onboardings en el espacio físico

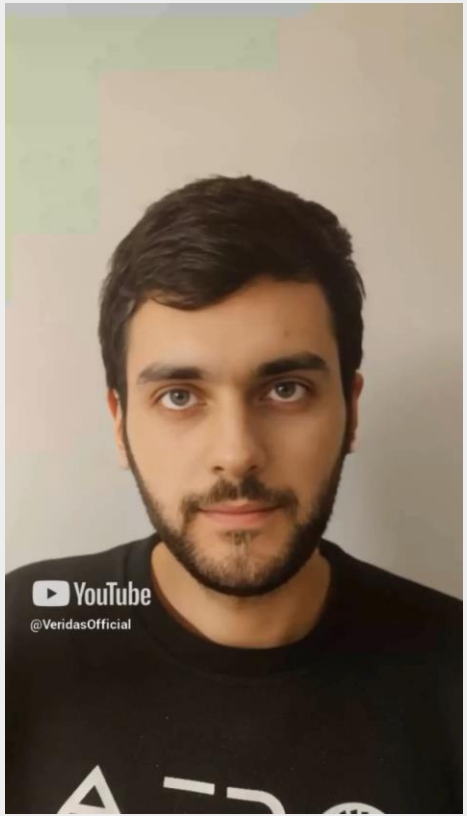
Un individuo se **registró más de 20 veces** en el mismo banco, pero **en diferentes sucursales**, utilizando documentos de identidad con otros nombres pero con una foto real de sí mismo.

/La nueva era del fraude de identidad
Los ataques de inyección

🚨 Casos reales de ataques de inyección detectados / Detección con emulador ⚠️

Un banco en Italia informó de varios intentos de **ataques de inyección**. El atacante generó un deepfake facial muy realista y lo introdujo en el sistema a través de un emulador. Los siguientes vídeos son ejemplos de los ataques realizados.

El banco confirmó que la solución Veridas detectó alrededor de 50 casos de fraude en solo dos semanas.



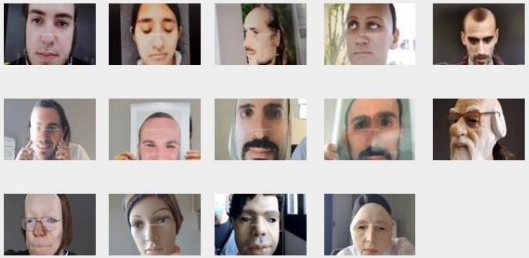
/La nueva era del fraude de identidad
Los ataques de inyección

/La nueva era del fraude de identidad
Los ataques de inyección

ANALOG ATTACKS | **DIGITAL** ATTACKS

Ataques de presentación

Intentos intencionados de engañar a los sistemas biométricos mediante la presentación de datos biométricos falsificados o alterados.



Cómo prevenirlos

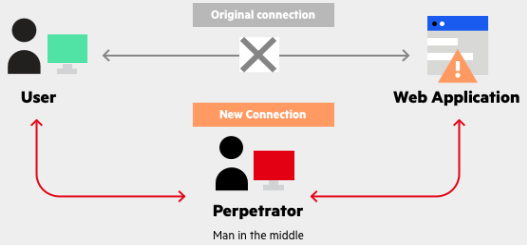
Implementación de una detección robusta de la vitalidad basada en técnicas de inteligencia artificial para distinguir los datos biométricos reales de los falsos.

Ataques de inyección

Introducción no autorizada de datos biométricos falsos en el proceso de autenticación

Man-in-the-middle Attack

Interceptación de la transmisión de datos biométricos durante la verificación



Cómo prevenirlos

Algoritmos avanzados de IA

/Ejemplos de fraude con IA generativa de voz
Máquina no engaña a máquina

VeriDas

¿Puedes identificar **cuál de estos audios se ha generado de forma sintética**?

Audio 1

Audio 2

Audio 3

La biometría
Un método controvertido

/La biometría. Un método controvertido

/Reglamento europeo de IA: un marco claro

TECNOLOGÍA	ESCENARIOS	RIESGOS
Reconocimiento biométrico	**Sistemas de identificación biométrica remota** (sin participación activa del usuario) **en tiempo real en espacios abiertos al público con fines policiales**	Prohibido con excepciones
	Sistemas de identificación biométrica remota (sin participación activa del usuario)	Alto
	Sistemas de identificación biométrica no remota (es decir, con participación activa del usuario)	Bajo o inexistente
	Sistemas de verificación biométrica	Bajo o inexistente
Categorización biométrica	**Sistemas de categorización biométrica que categoricen individualmente al individuo** basándose en sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliaciones sindicales, creencias religiosas o filosóficas, vida sexual u orientación sexual	Prohibido
	Sistemas de categorización biométrica empleando atributos sensibles o características basadas en la inferencia de dichos atributos	Alto
Inferencia de emociones	**Sistemas de inferencia de emociones en el lugar de trabajo o en instituciones educativas**	Prohibido con excepciones
	Sistemas de inferencia de emociones	Alto
Creación masiva de base de datos biométrica	**Sistemas para la creación o ampliación de bases de datos de reconocimiento facial mediante extracción masiva de imágenes faciales de internet o de imágenes de CCTV**	Prohibido

/La seguridad de la biometría

Los RBR ofrecen
una seguridad y una protección
de la privacidad inigualables
por defecto, en pleno
cumplimiento del RGPD

8. CONCLUSIONES

34. **La plantilla biométrica RBR** obtenida a partir de los rasgos (datos) biométricos es específica de una persona, pero **no es en absoluto única ni tampoco permanente**. Además, es **privada, irreversible, no interoperable, revocable y múltiple**.

35. Los mecanismos de control de acceso basados en la autenticación mediante comparación de una plantilla biométrica RBR dificultan la falsificación en comparación con otros métodos de autenticación, proporcionando una capa adicional de seguridad. **El factor de inherencia propio de la biometría** ofrece garantías de que la identidad es real, presentando ventajas significativas en comparación con factores de posesión o conocimiento que podrían ser cedidos o sustraídos por terceros.

36. El **reglamento europeo de Inteligencia Artificial**, que clasifica las aplicaciones de los sistemas de reconocimiento biométrico según el riesgo que puedan representar, califica las soluciones de **uso de la biometría** para el acceso con la intervención voluntaria del usuario y habitualmente en proximidad, **como de bajo o nulo riesgo** para los derechos fundamentales de las personas.

37. El Centro Criptológico Nacional recomienda para el nivel alto de seguridad el uso de **sistemas de control de acceso** basados en el uso de **plantillas biométricas RBR** (u otras que puedan surgir en un futuro que presenten protecciones equivalentes), **evaluados y certificados** conforme a las normas y estándares nacionales e internacionales sobre la materia.

/Cuánto se paga en la **dark web** por

Son mis Referencias Biométricas Renovables (RBR)

Identidad intrínseca (algo que soy)

Y no tengo miedo de compartirla ;)

0 €

Los ciberdelincuentes no pagan nada por los RBR

/”Tu cara no es única”

ISO 24745

Garantiza la privacidad de los datos protegiendo los datos biométricos de referencia

›

Privado

- No revela la identidad del usuario, a diferencia de un documento de identidad perdido.
- Los RBR se procesan de tal manera que no pueden vincularse a la característica biométrica original.

Irreversible

- No es posible reconstruir la imagen original, a diferencia de quien roba una contraseña o una foto de un carné de identidad.
- Los RBR son representaciones matemáticas que no pueden rastrearse hasta el rostro o la huella dactilar reales.

No interoperables

- No puede reutilizarse en otros sistemas, a diferencia de una contraseña que puede utilizarse para varias cuentas.
- Cada sistema genera un RBR único, por lo que es imposible utilizar la misma referencia en otro sistema.

Múltiple y Revocable

- Pueden sustituirse si se ponen en peligro, a diferencia de un documento de identidad perdido que puede utilizarse indebidamente.
- Los RBR pueden actualizarse o revocarse, lo que ofrece una forma segura de gestionar los datos biométricos en caso de compromiso.

Regulación

/España, referente en el mundo

BANCA

2016

SEPBLAC

Tecnología para el cumplimiento de las **Autorizaciones de verificación de identidad no presencial** (2016 y 2017)

AAPP

2021

Orden ETD/ 465/2021

Guía CCN-STIC-140, Anexo F.11

Métodos de identificación remota por vídeo para la **expedición de certificados electrónicos cualificados**

/eIDAS2

eIDAS 1

· Identidades notificadas.

· Servicios electrónicos de confianza:

  · Creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios..

  · Creación, verificación y validación de certificados para la autenticación de sitios web.

  · Preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

eIDAS 2

· **Wallet de identidad digital.**

· Servicios electrónicos de confianza:

  · Creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada, **atestación electrónica de atributos** y certificados relativos a estos servicios.

  · Creación, verificación y validación de certificados para la autenticación de sitios web.

  · Preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

  · **Archivo electrónico de documentos electrónicos**.

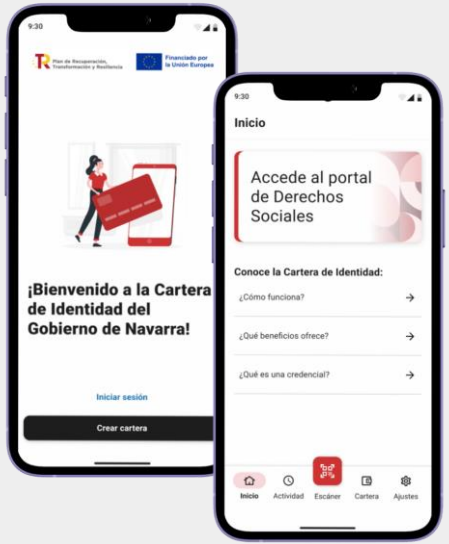
  · **Gestión de dispositivos de creación de firmas electrónicas remotas y de sellos electrónicos remotos**.

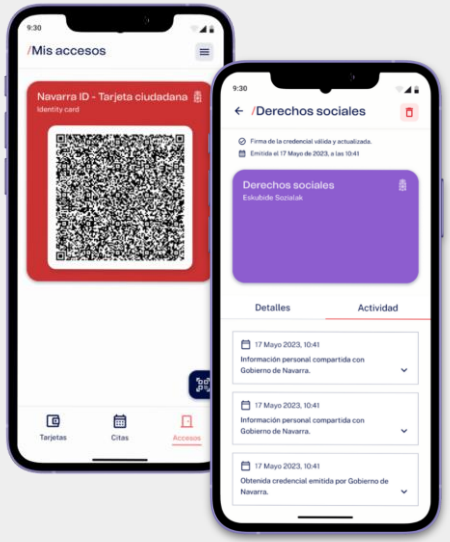
Seguridad, eficacia y transformación digital real

Casos reales

/Wallet de identidad
Una oportunidad histórica para Europa

Nafarroako Gobernua
Gobierno de Navarra





/Wallet de identidad
En uso para la ciudadanía en solo 30 días

Wallet
APP/SDK

/Espacio en el que almacenar credenciales verificables según el framework europeo de Verifiable Credentials.

Emisión de credenciales

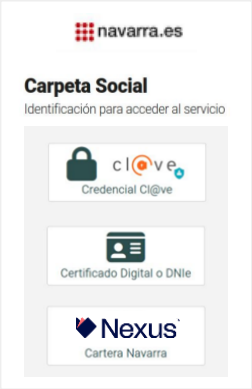
/Emisión de credenciales “madre” y derivadas tras un proceso robusto de alta de ciudadano.

/Personalización de credenciales con branding de servicio

Verificación de credenciales

/Conexión del wallet del usuario con servicios externos

/Verificación credenciales de acuerdo con el framework europeo



Integración sencilla

/Plugin de fácil integración del sistema de identidad en webs y apps. Conexión automática con servicios de emisión y verificación de credenciales y el wallet

/Haz login con NEXUS

/Wallet de identidad
Una oportunidad histórica para Europa

Pago de tributos sin contraseñas ni códigos... ¡y sin fraude!

Consultas ciudadanas digitales y seguras

Acceso passwordless a los servicios digitales gubernamentales

Alta online con la mejor experiencia de usuario

Acceso facial a los espacios físicos

/Verificación de identidad para emisión de certificados digitales

Acceso a
la carpeta de Salud

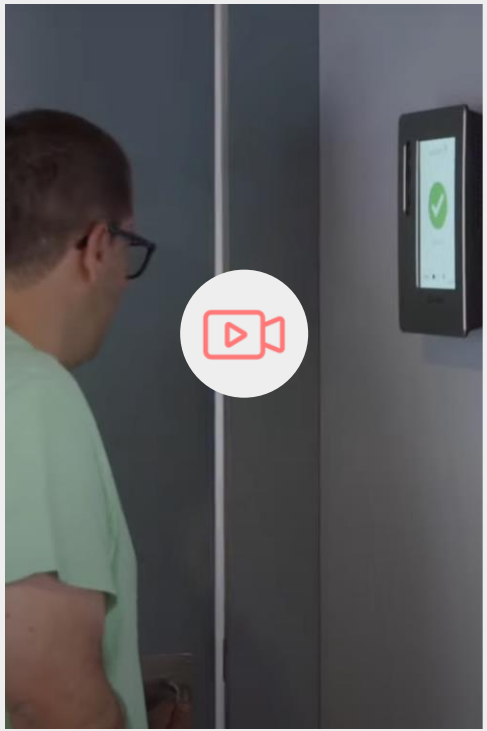
Denuncias online

Preinscripción escolar

Expedición de ID card para
firmar y tramitar solicitudes
con la AAPP

Solicitar Certificado Digital
Validación de identidad
Descargar e instalar certificado

/Reduciendo la brecha digital a través de la cara



PROBLEMA

A los usuarios de la Residencia San José no se les permitía abrir sus habitaciones por sí mismos, pese a tener plena capacidad de hacerlo. La seguridad y privacidad de las habitaciones prevalece sobre su propia capacidad.

RESULTADOS

> *Me agradó, porque era una forma en la que mi hermana tuviera su propia autonomía y su privacidad cuando ella quisiera. Como nos ocurre a todos.*

SOLUCIÓN

Apertura de puerta mediante biometría facial para entrar y salir de la habitación.

Acceso biométrico

/Eliminar el fraude de identidad en Servicios Sociales

EL PAÍS

ESTAFA >

Un hombre estafa más de un millón de euros en ayudas sociales en Bizkaia con 62 identidades falsas

La operación de la Policía Nacional se salda con la detención de 23 personas que participaban en la red

Pasaportes, tarjetas de crédito, libretas bancarias y teléfonos móviles, entre otros efectos, intervenidos durante la operación. POLICÍA NACIONAL

Passports, credit cards, bank books and mobile phones, among other effects, seized during the operation. NATIONAL POLICE

EJEMPLO REAL

Un solo individuo, múltiples onboardings en el espacio físico

Un individuo se **registró más de 20 veces** en el mismo banco, pero **en diferentes sucursales**, utilizando documentos de identidad con otros nombres pero con una foto real de sí mismo.

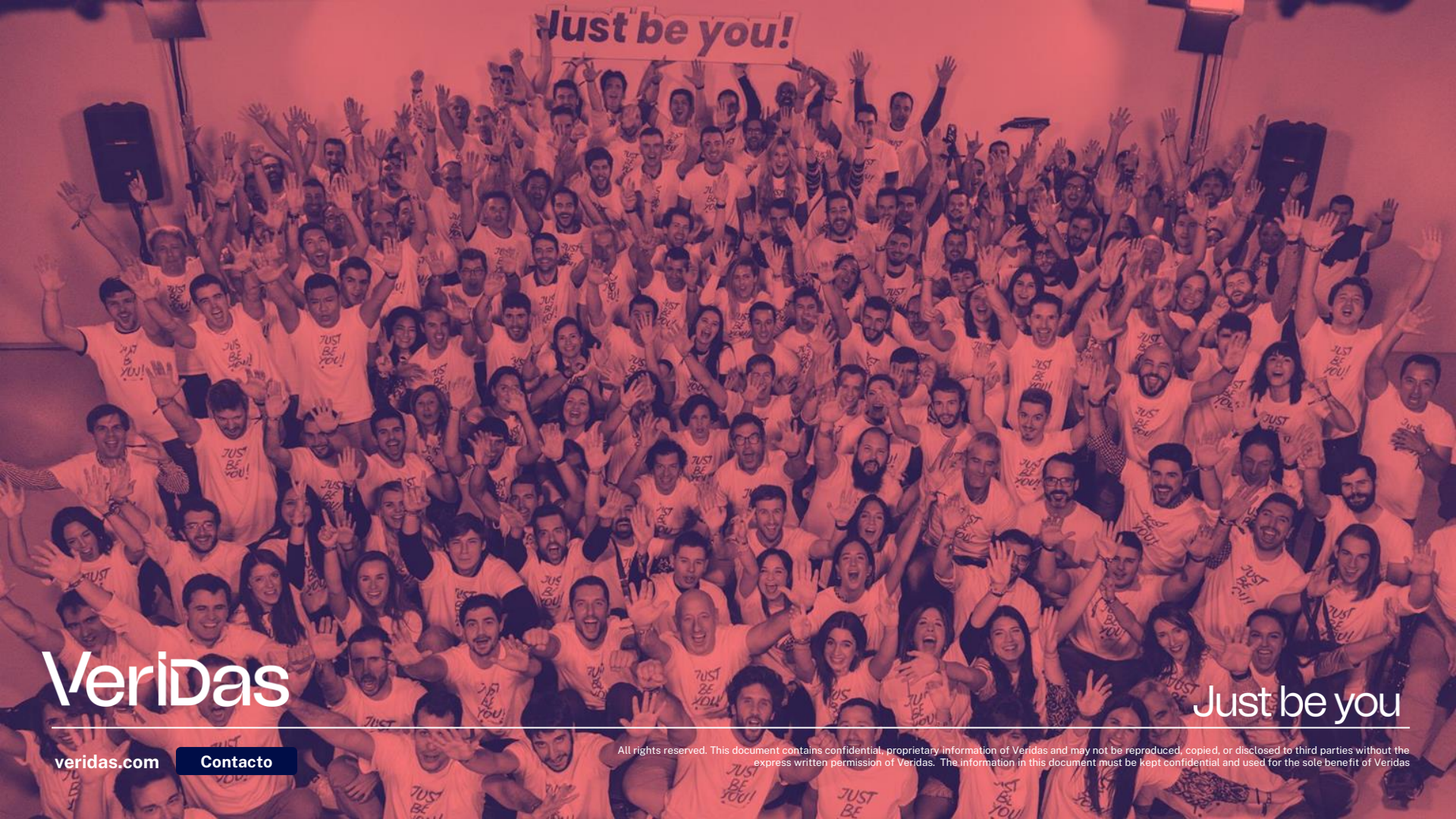
¿Cómo detectar a un defraudador que ha superado las medidas antispoofing desplegadas en oficinas?

15 minutos

25 ataques de fraude detectados

2000 nuevos usuarios

Eduardo Azanza
CEO / Veridas
eazanza@veridas.com



Veridas

Just be you

veridas.com

Contacto